International Journal of Power and Energy Systems, Vol. 45, No. 10, 2025
An Open Access Paper

RISK DETECTION IN THE WHOLE PROCESS OF POWER MONITORING HOST OPERATION BASED ON FUZZY LOGIC

Meijiao Xu,* Wei Ji,* and Wei Zhang*

Abstract

To realise the comprehensive dynamic detection of the risk of the whole process of power monitoring host operation, this study investigates a fuzzy logic-based risk detection method for the whole process of power monitoring host operation. The risk index design method, based on improved hierarchical analysis, is employed to develop threat probability and impact indices encompassing the complete host operation process. Subsequently, a risk event sequence clustering method utilising K-means clustering is applied to identify the sequence of risk events covered by these indices throughout the host operation process. According to the mined event sequences, a risk reasoning model for the entire host operation process is developed using a fuzzy logic-based approach, which combines affiliation degree and fuzzy rules to deduce risks in power monitoring and control. The risk inference model infers the risk intensity of the event sequences, thereby completing the risk detection for the entire host operation process. Experimental results demonstrate that this method accurately detects intrusion risks from single and mixed attacks throughout the power monitoring host operation process, with a risk detection delay of only 2 s, ensuring timely detection. In the clustering of risk event sequences, the clustering value for sequences under the threat probability index is set to 25, while the value of clustering the dangerous event sequences under the threat impact index is set to 20.

Key Words

Fuzzy logic, power monitoring, host, the whole process of operation, risk detection, index

1. Introduction

With the rapid development of computer and network technology, the development level of power system informatisation has also improved; however, this progress has simultaneously introduced numerous security vulnerabilities. According to relevant data, in recent years, network security management in the field of electric power has faced persistent invasion events involving the Stuxnet virus and Havex virus, which directly threaten the security of power monitoring hosts [1]–[3].

The power monitoring system serves the function of monitoring field equipment and alerting faults. If the host computer of the power monitoring system is invaded by a virus during operation, or if security measures are inadequately implemented, it may lead to the abnormal functioning of the power monitoring system, potentially impacting the operational status of the power system. Therefore, ensuring the security of the power monitoring system's host computer throughout its operational lifecycle is a critical task for the security department. Risk detection, an effective technique commonly employed at present, can analyse the operational status of the host throughout its lifecycle.

When detecting risks during the whole operation process of the power monitoring host, effective risk detection methods are necessary to protect the security of the host. Currently, numerous studies focus on risk detection for power monitoring mainframes. Based on the research results of others, Chai *et al.* [4] combined K-means clustering with a self-encoder to construct a host intrusion detection model, which extracts data samples by clustering host network traffic and identifies abnormal traffic through a self-encoder. While this method demonstrates more accurate host network intrusion detection capability, it is limited to detecting host operation risk through network traffic, restricting the factors that can be used to identify the risk. Yang *et. al,* [5] used attack graphs to assess host security. This method has been demonstrated to accurately assess the importance and security value of hosts, but the processing of attack graphs is complex. The accuracy of host risk detection results remains to be validated when the host is subjected to various attacks. Current research and discussions have primarily focused on traditional intrusion detection systems (IDS) and Intrusion prevention systems (IPS), employing techniques such as rule-based analysis, statistical analysis, and machine learning. These methods are typically used to detect

* State Grid East Inner Mongolia Electric Power Supply Co., Ltd., Hohhot, Inner Mongolia 010020, China; e-mail: {dengmeizong1oi, jiaokeng85855, que67482701}@163.com
Corresponding author: Meijiao Xu

Recommended by Zbigniew Leonowicz
(DOI: 10.2316/J.2025.203-0585)

malicious behaviours and security events in networks and attempt to identify potential intrusions. However, with the development of information technology and the increasing complexity of network environments, traditional intrusion detection methods face several challenges and limitations. For example, traditional methods may not accurately identify and categorise new intrusion methods and unknown threats. Furthermore, large-scale network traffic and dynamic network topologies can increase the complexity and difficulty of detection.

In this paper, a risk detection method based on fuzzy logic in the whole operation process of power monitoring host is proposed, which provides effective assistance for the safety protection of power monitoring host. In this paper, the method designs risk indicators by improving the hierarchical analysis method and evaluates the risk intensity by using the risk inference model of fuzzy logic, so as to realise the comprehensive and accurate detection of the operation risk of power monitoring and control mainframe. Compared with existing research, the advantage of this method is that it not only considers the threat probability and threat impact, but also introduces threat intelligence information and constructs a dynamic weight indicator system. Thus, it can more accurately reflect the risk status of the power monitoring host and provide effective support for security protection. The research contribution of this paper as follows.

(1) *Design Comprehensive Risk Assessment Indicators:* Improve the analytic hierarchy Process and design threat probability indicators and threat impact indicators that cover the entire process of host operation. Traditional methods often only consider the probability and impact of equipment failures, ignoring the complexity of equipment relationships and operational processes. The new indicators evaluate the possibility and severity of risks from multiple aspects such as threat mode, protection status, and host operation status, which can more accurately assess the operational risks of power monitoring hosts.

(2) *Mining potential risk event sequences:* Based on K-means clustering algorithm, cluster analysis is conducted on threat probability indicators and threat impact indicators to mine potential risk event sequences. This clustering method uses Euclidean distance as an indicator and determines the optimal number of clusters through contour coefficients. It can identify event sequences with similar risk characteristics, which helps to more accurately evaluate the risk situation.

(3) *Consider risk uncertainty assessment:* Construct a fuzzy logic based inference model, combined with membership degrees and fuzzy rules, to infer the risk intensity of risk event sequences. Traditional risk assessment methods often use simple mathematical models without considering the fuzziness and uncertainty in the assessment process. And this model can integrate multiple risk indicators, infer and detect risk intensity based on fuzzy rules, and more accurately evaluate the operational risks of power monitoring hosts.

2. Risk Detection Method in the Whole Operation Process of Power Monitoring Host

The fuzzy logic-based risk detection method for the whole process of power monitoring and control mainframe operation is mainly divided into three steps: the design of risk indicators for the whole process of power monitoring and control mainframe operation, the clustering of the sequence of risk events for the whole process of power monitoring and control mainframe operation [6], and the fuzzy inference of the risk level of the sequence of risk events.

2.1 Risk Index Design Method Based on Improved Analytic Hierarchy Process

Threat patterns and poor protection are important factors in assessing risk. Understanding existing threat patterns and potential attack patterns can help to identify the risk indicators to be used and on which to base a risk analysis [7]. A comprehensive understanding of existing protections and security policies is also required to identify weaknesses and vulnerabilities in the system. The entire operation of the power monitoring mainframe is analysed in detail, including data flow, system components and related processes. This helps identify possible risk points and key risk indicators. In order to comprehensively detect various risk factors in the whole process of power monitoring and control mainframe operation, this paper introduces the hierarchical analysis method, which is a complex method of analysing indicator weights [8]. However, in the risk detection of the whole process of power monitoring and control mainframe operation, if some mainframe risk detection indicators are significantly different from the normal value, it means that the risk value of the indicator is significant. However, the whole process of host operation is dynamic, and if the fixed weight method is used to detect the risk value, the dynamic risk intensity of the indicator cannot be accurately identified [9]. Therefore, this paper introduces the dynamic weight method to improve the hierarchical analysis method. With the application of the improved hierarchical analysis method, the weights of the risk indicators in the whole process of host operation will change with the dynamic change of the indicator values. If the state of the risk metrics during the whole process of host operation is abnormal, the corresponding weights will also change abnormally [10].

Risk metrics can be constructed based on known threat patterns and attack methods, but they may not cover all complex attack scenarios. This is because compound attacks may have new combinations or exploit unknown vulnerabilities. As a result, individual risk metrics may face inaccurate or unrecognisable detection in the face of composite attacks. To address this problem, a composite risk assessment approach can be considered that combines many different risk indicators. This can increase the coverage of attack detection and improve the detection of complex attacks.

The operational process for the risk index design method, based on the improved analytic hierarchy process, is as follows.

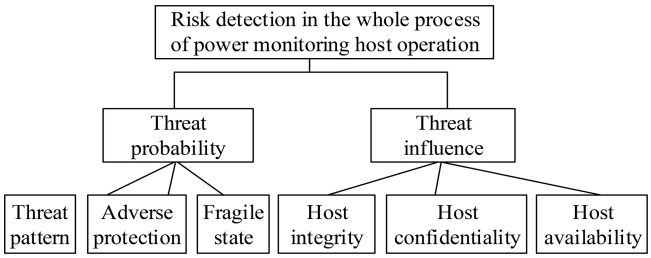

Figure 1. Risk indicators of the whole process of host operation.

Utilising the expertise and empirical knowledge of specialists in the field of power monitoring host security protection, the risk indicators pertaining to the comprehensive process of power monitoring host operation are delineated, as illustrated in Fig. 1.

As shown in Fig. 1, the risk indicators for the whole process of power monitoring and control host operation are mainly categorised into threat probability and threat impact. The core factors of the threat probability indicator are threat mode, unfavourable protection and vulnerability state. Threat mode mainly refers to the types of risks that occur during the whole process of host operation, such as abnormal access and vulnerability attacks. Unfavourable protection refers to the protection state of the host, and vulnerable state refers to the operating state of the host under risky operating conditions. The core factors of the threat impact indicators are mainly the integrity, confidentiality and availability of the host, which mainly describes whether the functionality of the host is impaired [11], whether the information security is threatened, and whether the host can operate normally. The design steps of risk indicators in the whole process of host operation are as follows.

(1) *Design of Judgement Matrix:* The pairwise comparison method is adopted to compare the criticality between the low-level influencing factors and the high-level factors in the whole operation process of the power monitoring host. The criticality is analysed by a nine-point scoring method [12]. Combined with the comparison results of each factor's criticality, and following the standard content shown in Table 1, the comparative relationship between risk influencing factors in the whole process of power monitoring host operation is transformed into the corresponding $m \times m$ hierarchical judgement matrix B.

(2) The sum product method is introduced to calculate the maximum characteristic root $\alpha_{\max}$ and the approximate value V of the maximum characteristic vector of the criticality judgement matrix of each influencing factor.

(3) Standardisation will be performed by using the following formula:

$$\overline{b}_{\mathrm{ij}} = \alpha_{\max} \sum_{i=1}^{m} b_{\mathrm{ij}} V \tag{1}$$

where $\overline{b}_{\mathrm{ij}}$ is the judgement matrix after standardisation, $b_{\mathrm{ij}} \in B$, which represents the judgement matrix of the criticality of risk influencing factors in the whole process of host operation in line i and column j in B.

Table 1
Contents of Nine-Point Standard

Scale	Details
1	Compared with the two influencing factors, the key degree is consistent
3	Compared with the two influencing factors, the first factor is slightly more critical
5	Compared with the two influencing factors, the first factor is more critical
7	Compared with the two influencing factors, the first factor is more critical
9	Compared with the two influencing factors, the first factor is very critical
2,4,6,8	Median values of scales 1, 3, 5, 7 and 9

(4) The critical judgement matrix of influencing factors after standardisation is summed [13]

$$U = \sum_{j=1}^{m} \overline{b}_{\mathrm{ij}} \varpi \tag{2}$$

where ϖ is the weight value.

(5) Calculate the approximate value of the principal eigenvector subsequent to the standardisation of the judgement matrix pertaining to the critical degree of influencing factors in line i

$$U_i = U \sum_{i=1}^{m} \iota_i \tag{3}$$

where ι_i is the sorting weight of line i.

(6) Perform consistency detection on the critical degree judgement matrix of the influencing factors of risk in the comprehensive process of host operation, and establish the consistency index as DJ

$$DJ = \frac{U_i}{m-1} \tag{4}$$

When the DJ value is close to 0, it represents significant consistency, but the matrix dimension is large, and it is difficult to control consistency [14]. m is dimension. Therefore, the average consistency index DS is used to detect the criticality of risk influencing factors throughout the host operation process to evaluate the consistency of the matrix, and there are

$$DS = \frac{\mathrm{DJ}}{m} \tag{5}$$

If the value of DS exceeds 0.15, the consistency of the judgement matrix of influencing factor criticality is significant; otherwise, if it is less than 0.15, the consistency is not significant, so it is necessary to jump to step (1) and form a new judgement matrix again [15].

(7) Check the consistency of the total ranking of levels: For the purpose of calculating the weight of a certain level factor relative to the highest level, the total ranking of levels is performed. If the number of influencing factors in the whole process of host operation risk in B at the upper level is n, the weight of total ranking at the lower level is $(\iota_1, \iota_2, ..., \iota_i)$, the number of factors in C is m, and the ranking weights of B_i and C_i factors are ι_B and ι_C in turn, the hierarchical consistency test is carried out

$$DS = \frac{\sum_{j=1}^{n} \iota_C \times DJ_j}{\sum_{j=1}^{n} \iota_B \times SJ_j} \tag{6}$$

In the formula, DJ_j and SJ_j are the consistency detection index and random consistency index of layer C_j factor and upper layer B_j in turn.

If the value of DS is not greater than 0.15. Then the consistency of the ranking results of influencing factors' criticality levels is significant [16], otherwise, skip to step (1).

(8) Build a dynamic weight index system: Setting the initial weight of the index to which the risk influencing factors in the whole process of host operation belong to ζ, and establishing a dynamic weight function X corresponding to the risk index

$$X = DS\zeta \sum_{l=1}^{m} g_l \beta \tag{7}$$

where g_l is the dynamic weight of the l risk indicator and β is the host level protection coefficient. When the X value is greater than 1, it indicates that the risk of the host is high [17], and it is necessary to detect the operation of the host in time.

2.2 Risk Event Sequence Clustering Method–based on K-means Clustering

According to the risk index constructed in Section 2.1, the risk event sequence of the whole operation process of the power monitoring mainframe is extracted by using the K-means clustering algorithm. The K-means clustering algorithm mainly uses the Euclidean distance as an index, and the number of clusters of the risk event sequence of the operation of the power monitoring mainframe is set as k .The clustering process is as follows.

(1) Randomly extracting $k$operation risk event sequence samples in the whole operation process of the power monitoring host, and setting these samples as an initial clustering center $o = (o_1, o_2, ..., o_k)$;

(2) Set the operating risk event sequence set of the power monitoring host. The i risk event sequence sample is θ_i, calculate its distance from $o = (o_1, o_2, ..., o_k)$, and classify θ_i into the cluster E_i to which the cluster center with the smallest distance belongs

$$E_i = X \underset{j}{\operatorname{argmin}} \left\| \theta_i - o_i \right\|^2 \tag{8}$$

In the formula, o_i is the i cluster center in k risk event sequence.

$$o_i = \frac{1}{|E_i|} \sum_{i=1}^{n} \theta_i \tag{9}$$

Step (2) is executed several times, and the clustering of the risk event sequence of the power monitoring host can be stopped when the change of the clustering center is minimum or fixed [18], [19]. The algorithm is unable to set the number of clusters of risk event sequences during operation [20], so this paper introduces the profile coefficients based on cohesion and separation to set the number of clusters k. First, the average distance between the j risk event sequence target and its in-class event sequence is ϕ_j, and the average distance between the j risk event sequence target and other cluster event sequences is φ_j. For the j risk event sequence, its contour coefficient is set as [21]

$$r_j = \frac{\varphi_j - \phi_j}{o_i \max(\phi_j, \varphi_j)} \tag{10}$$

Then the clustering contour coefficient of all risk event sequences in the whole process of power monitoring host operation is

$$r = \frac{1}{m} \sum_{j=1}^{m} r_j \tag{11}$$

The maximum value and minimum value of r are 1 and 0 in turn. If the value of r is not less than 0, the clustering effect of risk event sequence of power monitoring host is excellent. The closer the value of r is to 1, the smaller the intra-class distance and the larger the inter-class distance after clustering, and the clustering quality of risk event sequence is remarkable. On the contrary, if the value of r is less than 0, the clustering effect is not good [22].

2.3 Risk Reasoning Model of the Whole Process of Host Operation Based on Fuzzy Logic

The host risk event sequence, derived through clustering in Section 2.2, is imported into the risk reasoning model for the comprehensive host operation process based on fuzzy logic. Subsequently, the risk intensity of the event sequence is evaluated using fuzzy reasoning techniques.

The structure of the risk reasoning model for the whole process of host operation based on fuzzy logic is shown in Fig. 2.

The model can combine the actual host risk level requirements to comprehensively infer the risk intensity of the whole process of power monitoring and control host operation. As shown in Fig. 2, the model can combine multiple risk indicators in Section 2.2 and follow fuzzy rules to infer and detect the risk intensity of the sequence of risk events in the whole process of host operation.

The fuzzy logic-based risk inference model for the whole process of host operation sets the risk intensity level to the criteria shown in Table 2 when inferring the risk intensity.

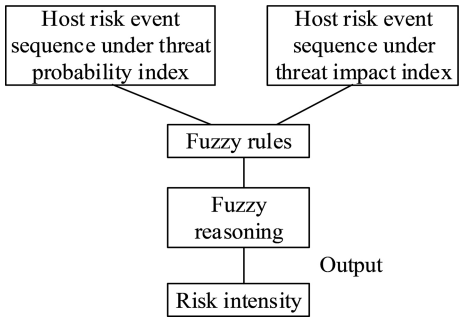

Figure 2. Risk reasoning model of the whole process of host operation based on fuzzy logic.

Table 2
Risk Intensity Levels

Risk intensity	Grade of membership
Polar altitude	0.81∼1.00
Height	0.61∼0.80
Moderate	0.41∼0.60
Minuent	0.21∼0.40
Very low	0.00∼0.20

Fuzzy rules mainly use IF-THEN method to construct the relationship between risk indicators and risk intensity, and combine with the index membership function set by experts to construct fuzzy rules [23]. Examples of fuzzy rules as follows.

(1) From the threat probability and threat impact of the risk indicators shown in Fig. 1, if the threat probability and risk impact are acceptable, then the degree of risk affiliation of the power monitoring and control mainframe throughout the operation is 0.00∼0.20.
(2) If the threat probability and threat impact belong to the high-risk category, then the affiliation degree of the risk degree in the whole operation process of the power monitoring host is 0.61∼0.80.

Threat probability cannot directly determine the risk detection result of the whole process of host operation, but threat impact has some influence on the risk detection effect of the whole process of host operation, because there are some defense measures in the whole process of host operation, so the threat impact index is the core index that ultimately reflects the risk of the whole process of host operation [24]. The applicability of fuzzy logic and K-means based detection methods as well as the clarity of the execution process can be improved by combining other machine learning techniques, investigating precise risk metrics, introducing threat intelligence information, implementing comprehensive assessment and testing, and enhancing interpretation and visualisation. These solutions can provide more accurate, reliable and effective detection mechanisms to fulfill the security requirements for the entire operation of power monitoring hosts.

3. Experimental Analysis

In order to test whether the method in this paper has the capability of risk detection in the whole process of power monitoring host operation, the network environment of the power monitoring host is designed on the virtualisation software Vmware workstation for experimentation, and three intrusion behaviours are used to simulate the risk problems in the whole process of host operation. The information of intrusion behaviours is as follows.

Behaviour 1: ARP attack on the power monitoring host through Kali Linux;

Behaviour 2: Host manipulation vulnerability attack on Winserver;

Behaviour 3: Host DOS attack.

Behaviour 1 and Behaviour 3 require the use of Kali Linux commands to drive arpspoof and hping3 to complete the host intrusion; Behaviour 2 is the use of Kali Linux commands to complete the vulnerability attack through the vulnerability of the target Windows 10 operating system.

When using Vmware-workstation 12.0 to build the virtual experimental environment, the virtual network topology is divided by subnetting, and the subnet mask is set to 255.255.255.0, which divides multiple subnets, each of which corresponds to a different experimental equipment role. The subnet where the power monitoring host is located, the subnet where the attack source is located, and so on. The virtual host hardware parameters are configured to allocate 2 CPU cores, 4 GB of RAM, and 20 GB of hard disk space for the power monitoring host. For the Kali-Linux 2021.2 simulated attack behaviour, the network attack tool that comes with it is used to realise the attack function through a specific combination of command line parameters. The Windows 10 operating system (version 1803 - 17134.191) is used as the operating system of the power monitoring host in the experiments, and the network parameters are configured as the static IP address 192.168. 1.100, subnet mask 255.255.255.0, default gateway 192.168.1.1, and necessary services are enabled to simulate the actual operating environment. Set the capture filter to capture only the network protocol packets related to the experiment, such as ARP, TCP, UDP, *etc.* Use data cleaning technology to remove duplicate and wrong packets, and extract key features such as source IP, destination IP, port number, protocol type, *etc.,* of the packets through feature extraction algorithm.

Table 3 shows the details of the software used in the experiment and the simulation behaviour.

Based on the set experimental environment, taking Behaviour 1 as an example and incorporating the risk index for the comprehensive power monitoring host operation process delineated in Fig. 1, the method in this paper demonstrates significant importance in mining the risk event sequence of the whole process of power monitoring system host operation. Figure 3 shows the clustering effect of the risk event sequence in the whole process of host operation under different clustering conditions, with the clustering effectiveness primarily quantified by the silhouette coefficient.

Table 3
Details of Software and Simulation Behaviour Used in the Experiment

Software type	Version	Function
Virtualisation software Vmware-workstation	12.0	Design the virtual experimental environment of power monitoring host
kali-Linux software	2021.2	Simulate attack behaviour
Windows 10 operating system	1803-17134.191	Operating system
Windows 10 Physical machine	Memory 8G, clocked at 3.0GHZ	Code writing, resource allocation
Wireshark	3.6.6.0	Data parsing
Adobe Reader	4.0	Vulnerability management

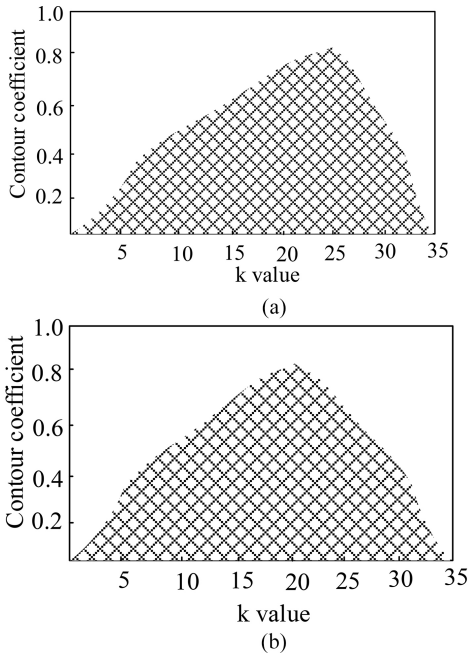

Figure 3. Relationship between cluster of risk event sequence and contour coefficient: (a) Mining effect of risk event sequence under threat probability index and (b) Mining effect of risk event sequence under threat impact index.

Figure 3 illustrates the relationship between the cluster number k and the contour coefficient of the risk event sequence, represented on the horizontal and vertical axes, respectively. A larger contour coefficient indicates a more significant clustering effect of the risk event sequence for a given k value. In the category of risk index-threat probability, the contour coefficient reaches its maximum when k equals 25 after clustering the risk event sequence. In the category of risk index-threat impact, the contour coefficient attains its peak when k equals 20 after clustering the risk event sequence. Consequently, when clustering the risk event sequence, the k value of the risk event sequence cluster under the threat probability index is set to 25, and the k value of the risk event sequence cluster under the threat impact index is set to 20.

After clustering the risk event sequence of the whole operation process of the power monitoring system, this method employs a risk inference model based on fuzzy logic to assess the risk intensity of the aforementioned sequences. The detection result fed back by this method in the virtualisation software Vmware-workstation is shown in Fig. 4.

As shown in Fig. 4, after the method of this paper detects the risk intensity of the whole process of power monitoring host operation, the detection results show that the risk intensity of the whole process of host operation is moderate, which is mainly reflected in the following factors: threat mode, unfavourable protection, vulnerable state, host integrity, confidentiality and availability. The risk intensity affiliation of the host risk event sequence is 0.10, 0.05, 0.10, 0.05 and 0.10, respectively.

Under the attack of behaviour 1, experimental conditions of different risk intensities are simulated. The detection accuracy of the method in this paper is analysed when it detects the whole process risk of host operation for many times. The results are shown in Fig. 5.

As shown in Fig. 5, the method presented in this paper demonstrates a high degree of correlation between the detected risk and the actual risk intensity in the power monitoring system host operation process. The detection results exhibit a positive linear correlation trend and consistently exceed the reference line, indicating that this method is effective for risk detection in the power monitoring host operation process.

The specifics of risk intensity over time are recorded for ARP attacks, host manipulation vulnerability attacks, host DOS attacks, and hybrid attacks, respectively. The graph visually compares how the risk intensity evolves over time under different attack scenarios, and verifies the capability of this paper's approach in real-time monitoring and risk assessment. The graph of risk intensity over time under different attack behaviours is shown in Fig. 6.

From Fig. 6, it can be seen that the risk intensity increases with time under different attack behaviours. At

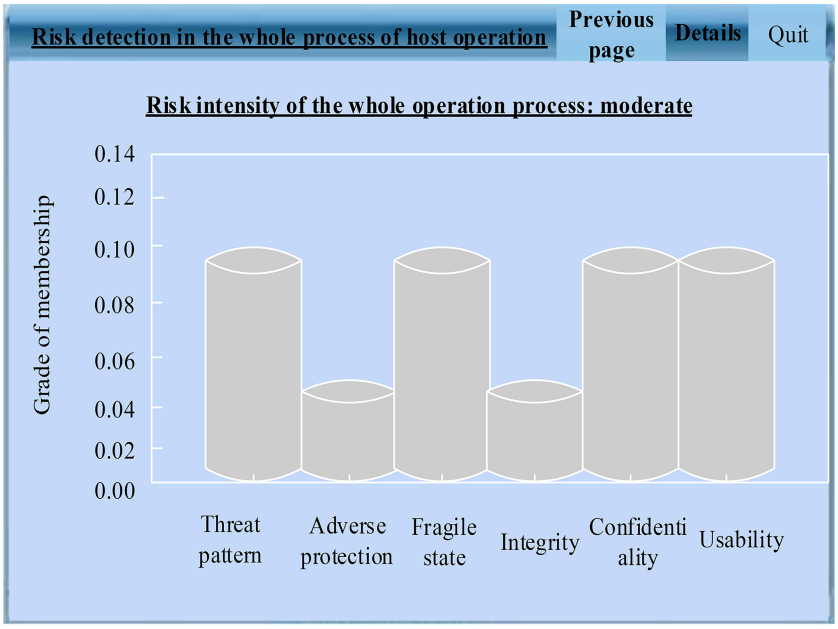

Figure 4. The detection result fed back by this method.

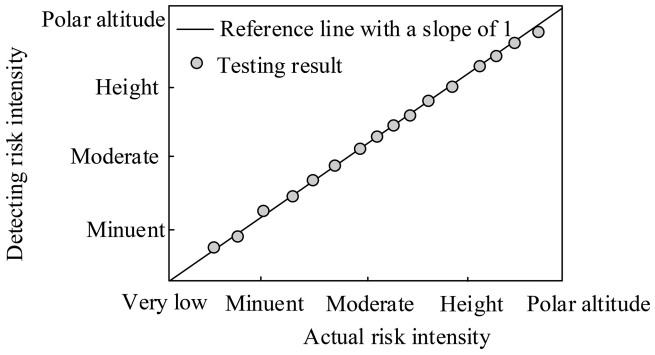

Figure 5. Risk detection accuracy test results.

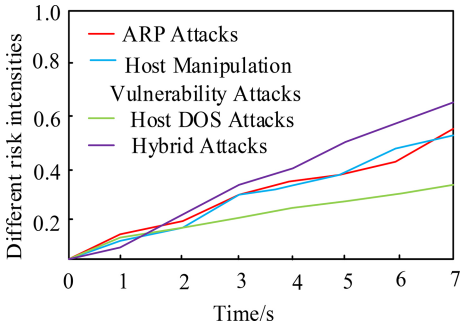

Figure 6. Plot of risk intensity over time for different attack behaviours.

the initial moment, the risk intensity of all types of attacks is low and similar. As time passes, the risk intensity of hybrid attacks increases most significantly and reaches a high level at 7 s. The risk intensities of ARP attacks, host manipulation vulnerability attacks, and host DOS attacks also increase gradually, but the growth rate and speed are relatively small compared to that of hybrid attacks. This shows that the method can effectively monitor the change of risk intensity under different attack behaviours in real time, and verifies that the impact of multiple attack behaviours on the risk of host operation is dynamically intensified.

Table 4
Detection Effect of Mixed Attack Behaviour

Types and time of attack behaviour	Detection results and detection time of this method
Behaviour 1 + Behaviour 2: October 5, 2021 09: 45: 00	ARP attack + vulnerability attack Winserver: October 5, 2021 09:44:58
Behaviour 1 + Behaviour 3: October 5, 2021 09:50:00	ARP attack + DOS attack: October 5, 2021 09:49:58
Behaviour 2 + Behaviour 3: October 5, 2021 09:55:00	Vulnerability attack Winserver + DOS attack: October 5, 2021 09:54:58

To evaluate the efficacy of this method in detecting mixed attacks, a test was conducted during the setup of the power monitoring host, wherein multiple types of attacks occurred simultaneously. The results of this evaluation are presented in Table 4.

As shown in the test results in Table 4, the risk detection results of mixed attack behaviour within the same time period throughout the power monitoring host operation process using this method align with the actual situation, exhibiting high detection accuracy, precise risk intensity detection results, and notable real-time detection capabilities. When risk behaviour appears for 2 s, this method can complete the risk detection across the whole process of power monitoring host operation.

To further verify the effectiveness of the proposed method, a comparison is conducted using known data

Table 5
Comparison of False Alarm Rates of Different Detection Methods

Number of iterations	Textual method %	Unsupervised host intrusion detection method based on EKM-AE model %	Host security evaluation method based on attack graph %
10	6.42	16.62	14.98
20	6.35	14.25	16.26
30	5.42	17.42	13.64
40	4.15	19.36	14.55
50	3.47	17.15	13.64
60	3.15	16.26	17.46

Table 6
Performance Comparison Results of Different Detection Methods

Experimental indicators	Textual method	Traditional fuzzy logic approach model
F1 score	0.92	0.85
AUC	0.95	0.89
Kappa coefficient	0.88	0.79

sets between the proposed method, the unsupervised host intrusion detection method based on the EKM-AE model, and the host security assessment method based on attack graph. The test index is false alarm detection rate, and the specific comparison results are shown in Table 5.

As demonstrated in Table 5, the minimum false alarm detection rate of the proposed method is 3.15%, whereas the lowest false alarm detection rate of the unsupervised host intrusion detection method based on EKM-AE model and the lowest false alarm detection rate of the host security assessment method based on attack graph are 14.25% and 13.64%. Compared with the two literatures, the false alarm detection rate of the proposed method is lower.

Evaluate the performance of the risk detection method proposed in this paper compared to existing fuzzy logic methods in terms of F1 score, AUC, and Kappa coefficient. Through comparative experiments, verify the effectiveness and advantages of the proposed method in detecting operational risks of power monitoring hosts. The specific comparison results are shown in Table 6.

According to the comparison results in Table 6, the risk detection method proposed in this paper outperforms the traditional fuzzy logic method in three key performance indicators: F1 score, AUC, and Kappa coefficient. The F1 score of the method is as high as 0.92, which is a very high classification accuracy; the AUC value is 0.95, which indicates that it has a good model recognition ability; and the Kappa coefficient is 0.88, which indicates that the detection results have a high consistency with the actual situation. In summary, the risk detection method proposed in this paper has good performance in detecting the operational risk of power monitoring hosts and has significant effectiveness and advantages.

4. Result and Discussion

In this paper, the whole process risk detection of power monitoring host based on fuzzy logic is proposed and the following conclusions are drawn as follows.

1) When clustering the sequence of risk events, the value of clustering the sequence of risk events under the threat probability index is set to 25, and the value of clustering the sequence of dangerous events under the threat impact index is set to 20.
2) The risk intensity of the whole host operation process is moderate, which is mainly reflected in the threat mode, unfavourable protection, vulnerable state, host integrity, confidentiality and availability. The risk intensity affiliation of major risk events are 0.10, 0.05, 0.10, 0.05 and 0.10, respectively.
3) After detecting the risk in the whole operation process of the power monitoring host, the detection results are highly matched with the actual risk intensity, and there is a linear positive correlation trend, and the detection results are above the reference line, which indicates that the method in this paper can be used for the risk detection task in the whole operation process of the power monitoring host.

When the risky behaviour appears for 2 s, the method can complete the risk detection of the whole operation process of the power monitoring host.

5. Conclusion

The problem of risk detection in the whole process of power monitoring host represents a critical challenge that requires urgent resolution in the current safety management of power monitoring systems. This study proposes a risk detection method for the comprehensive operational process of power monitoring hosts based on fuzzy logic, with the aim of accurately and efficiently identifying risks during host operation. The efficacy of this method is evaluated through virtual simulation. The experimental results show that when clustering risk event sequences, setting the clustering value of the risk event sequence under the threat probability index to 25 and the value of the threat impact index to 20 yields the best clustering effect. This method detects a moderate level of risk throughout the entire process of host operation, mainly reflected in threat modes, adverse protection, fragile states, as well as the integrity, confidentiality, and availability of the host. The risk intensity membership degrees of each major risk event are 0.10, 0.05, 0.10, 0.05, 0.10, and 0.10, respectively. The detection results are highly matched with the actual risk intensity, showing a linear positive correlation and located above the reference line. The detection can be completed within 2 s of the occurrence of risk behaviour. The detection results for mixed attack

behaviour also conform to the actual situation, indicating that this method can be used for risk detection tasks throughout the operation of power monitoring hosts.

Because the reasoning and judgement involved in fuzzy logic are fuzzy, the results may be affected by the setting of key parameters and professional knowledge, resulting in a degree of uncertainty. In the complex and ever-changing power monitoring environment, subtle adjustments to key parameters or differences in understanding of knowledge among different professionals may cause changes in risk detection results, thereby affecting the accurate assessment and effective response to operational risks of power monitoring hosts. In future development, the integration of deep learning and machine learning technologies may enhance the system's capacity to analyse and interpret complex power monitoring data, potentially improving the accuray and robustness of risk detection mechanisms.

Data Availability

Data will be made available on request.

Acknowledgment

The study was supported by State Grid East Inner Mongolia Electric Power Supply Co., Ltd. through "Detection technology of host safety protection configuration in power monitoring system and the research and implementation of fast reinforcement method" (Grant No. SGMD0000DDJS2200049).

References

[1] Z. Liang, Q. Gang, L. Huixing, and J. Haochun, Research and application on key technologies of network security situation awareness platform of smart grid power monitoring system. *Journal of Shanghai Jiaotong University*, *55*(S2), 2021, 103–109.

[2] W. Jie, Z. Zhiming, and L. Chengbo, Research on perception of advanced persistent threat in power monitoring system, *Advances of Power System Hydroelectric Engineering*, *36*(5), 2020, 64–68+74.

[3] S. Yiding and L. Qiang. Towards discovering compromised hosts with temporal-spatial behaviours in advanced persistent threats, *Application Research of Computers*, *39*(6), 2022, 1860–1864.

[4] C. Yachuang, Y. Wenzhong, Z. Zhihao, H. Zhiquan, D. Huixiang, and Q. Yunyun, Unsupervised host intrusion detection method based on EKM-AE model. *Journal of Chinese Computer Systems*, *42*(4), 2021, 868–874.

[5] Y. Hongyu, Y. Haihang, and Z. Liang, Host security assessment method based on attack graph, *Journal on Communications*, 43(2), 2022, 89–99.

[6] P. Mundra, A. Arya, S.K. Gawre, Assessing the impact of renewable purchase obligation on Indian power sector, *International Journal of Power and Energy Systems*, *40*(4), 2020.

[7] L. Xuyang, N. Xin, H. Junxing, Y. Junfeng, and M. Han, Ensemble learning based malware detection method for smart gird. *Journal of Chongqing University (Natural Science Edition)*, *44*(3), 2021, 144–150.

[8] Y. Hongyu, Y. Haihang, and Z. Liang, A risk assessment method of network host node with host importance. *Journal of Beijing University of Posts and Telecommunications*, *45*(2), 2022, 16–21.

[9] Yangliuqing and W. Chong, Aload prediction based physical host status detection strategy in cloud data centers, *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)*, *33*(6), 2021, 1014–1023.

[10] D. Wei, Network security threat prevention and control system of electric power monitoring systems for wind farm. *Telecommunications Science*, *36*(5), 2020, 138–144.

[11] Q. Shengpan, Y. Yang, Z. Tianyi, Z. Xudong, and C. Yanbo, Research on online prediction model of host load based on deep learning. *Computer Engineering*, *47*(9), 2021, 84–89.

[12] G. Dezhi, X. Gan, High-dimensional mixed attribute data mining method based on K-means clustering algorithm. *Computer Simulation*, *38*(2), 2021, 308–312.

[13] L. Rong, and Z. Siwang, Power monitoring system based on compressive sensing. *Control Engineering of China*, *26*(5), 2019, 952–956.

[14] Y. Gang, Y. Yali, L. Hua, R. Dongwu, H. Junfe, and W. Fang, Development and application of reference data avalanche automatic test system of smart substation monitoring system, *Power System Protection and Control*, *47*(18), 2019, 182–187.

[15] L. Junwei, T. Yafang, H. Zhenghang, M. Guolong, and J. Youquan, Survey of cluster analysis and its application in power system, *Modern Electric Power*, 36(3), 2019, 1–10.

[16] Y. Zhiyuan, Z. Shipeng, S. Hao, and G.Xiohong, Risk estimation of cyber threat to substation based on cyber-net and learning algorithm. *Automation of Electric Power Systems*, *44*(24), 2020, 19–27.

[17] Z. Ying, W. Bin, and T. Ningshan. Risk assessment of power monitoring system based on cloud model and improved evidence theory. *Computer Systems Applications*, *31*(8), 2022, 55–63.

[18] A.A. Dubov, Risk monitoring based on early diagnosis of potential damage to power equipment, *Thermal Engineering*, *68*(9), 2021, 730–734.

[19] H. Li, T. Li, Q. Yao, W. Li, L. Yang, and G. Sun, Risk assessment of power monitoring system based on fuzzy analytical hierarchy process, *Journal of Physics: Conference Series*, *2137*(1), 2021, 012023.

[20] A. Hooshyar, Guest editorial special issue on resilience-oriented protection, control, and monitoring systems for power grids, *IEEE Transactions on Power Delivery*, *36*(4), 2021, 2251–2252.

[21] S. Mor, N. Vig, and K. Ravindra, Distribution of heavy metals in surface soil near a coal power production unit: Potential risk to ecology and human health, *Environmental monitoring and assessment*, *194*(4), 2022, 263.

[22] O. Behr, K. Barre, F. Bontadina, R. Brinkmann, M. Dietz, T. Disca, J. S. P. Froidevaux, S. Ghanem, S. Huemer, J. Hurst, S. K. Kaminsky, V. Kelm, F. Korner-Nievergelt, M. Lauper, P. Lintott, C. Newman, T. Peterson, J. Proksch, C. Roemer, W. Schorcht, and M. Nagy, Standardised and referenced acoustic monitoring reliably estimates bat fatalities at wind turbines: Comments on 'Limitations of acoustic monitoring at wind turbines to evaluate fatality risk of bats', *Mammal Review*, *53*(2), 2023, 65–71.

[23] M. Ahmad and R. Mohd-Mokhtar, Design of H-/H8 based fault detection filter for linear uncertain systems using linear matrix inequalities, *International Journal of Robotics and Automation*, *14*(2), 2025, 214–226.

[24] N.I.M. Azmi, and N. M. Yahya, Position tracking of DC motor with PID controller utilizing particle swarm optimization algorithm with Lvy flight and Doppler effect, *International Journal of Robotics and Automation*, *14*(1), 2025, 67–73.

Biographies

Meijiao Xu received the Master of Engineering degree from Inner Mongolia Agricultural University. She currently works as a Principal Engineer with State Grid East Inner Mongolia Electric Power Supply Co., Ltd. Her research directions include power dispatch automation, power system, and its automation.

Wei Ji received the Master of Engineering degree in electrical engineering from North China Electric Power University. He currently works as a Principal Engineer with State Grid East Inner Mongolia Electric Power Supply Co., Ltd. His research directions included power dispatch automation, power systems, and their automation.

Wei Zhang received the Master of Electrical Engineering degree from Northeast Electric Power University. He currently works as an Engineer with the State Grid East Inner Mongolia Electric Power Supply Co., Ltd. His research directions included power dispatch automation, power systems, and their automation.